UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,377	12/12/2001	Ashley Anderson Brock	RSW920010214US1	2825

26502 7590 02/14/2006

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/015,377	**Applicant(s)** BROCK ET AL.	
	Examiner Longbit Chai	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 January 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-32* is/are pending in the application.

4a) Of the above claim(s) *27-30* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-26,31 and 32* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 December 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1 – 20 have been presented for examination. Claims 1 – 20 have been canceled; new claims 21 – 32 have been added in an amendment filed 01/06/2006. Claims 27 – 30 have been withdrawn due to the restriction requirement. Therefore, presently pending claims for this instant application are 21 – 26 and 31 – 32.

Election / Restrictions

On February 7, 2006, discussed with attorney Arthur J. Samodovitz (Reg. No: 31,297) over the phone regarding restriction requirement resulted from the amendment filed on 01/06/2006. Attorney elects the first group (Group II) without traverse from the following two groups.

This application contains claims directed to the following patentably distinct claimed inventions. Restriction to one of the following invention is required under 35 U.S.C 121:

I. (Group I) Claims 27 – 30 drawn to an effective instruction detection method by storing the null signature of the system event, classified in class 726, subclass 23.

II. (Group II) Claims 1 – 26 and 31 – 32 drawn to a more specific instruction detection method that stores a plurality of intrusion signatures in an order based upon the frequency / likelihood of occurrence of signature matches, classified in class 726, subclass 25.

Inventions I and II are related as subcombination disclosed as usable together in a single combination. The subcombination is distinct from the combination and the subcombinations are distinct from each other if they are shown to be separately usable. The following case instants:

Invention I has separate utility directed to an effective instruction detection method by storing the null signature of the system event with an indication that no corrective action is needed in response to detection of said subsequent system event.

Invention II has separate utility directed to a more specific instruction detection method that stores a plurality of intrusion signatures in an order based upon the frequency / likelihood of occurrence of signature matches so that subsequently comparing a signature of a subsequent system event with said plurality of intrusion signatures in the corresponding order.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purpose as indicated is proper.

Examiner acknowledges that Applicant has elected Group II without traverse and as such this Office action only addresses the claimed inventions of Group II.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 31 – 32 recites the limitation "storing said one system event signature in association with said plurality of intrusion signatures". There is insufficient antecedent basis for this limitation in the claim, which appears as either (a) one of said system event signatures or (b) other of said system event signatures because both are qualified as <u>said one system event signature</u> in association with said plurality of intrusion signatures. More specific claim limitation is respectfully requested to overcome this rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 21 – 26 and 31 – 32 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya (U.S. Patent 6279113).

As per claim 21 and 24, Vaidya teaches a method of detecting intrusions said method comprising the steps of:

storing a plurality of intrusion signatures (Vaidya: Column 2 Line 53 – 59);

automatically detecting a multiplicity of system events having respective signatures (Vaidya: Column 3 Line 40 – 45);

comparing each of said multiplicity of system event signatures to said plurality of intrusion signatures (Vaidya: Column 4 Line 8 – 18);

recording a number of times that each of said intrusion signatures matched said system event signatures (Vaidya: Column 8 Line 18 – 39);

automatically ordering the stored plurality of intrusion signatures based on how many times each of said intrusion signatures matched said system event signatures, such that the intrusion signature matching the most system event signatures is first in the order (Vaidya: Column 11 Line 48 – 51: the likelihood of occurrence is based on the occurrence sequence of events during the network intrusion detection presented as in an sequential order on the list (table) of the attack signature profile – i.e. the first qualifier condition would be always can be met most of the time as the comparison goes by and stop anytime when not matched); and subsequently comparing a signature of a subsequent system event with said plurality of intrusion signatures in said order (Vaidya: Column 11 Line 48 – 51: see the same rationale as above).

As per claim 22 and 25, Vaidya teaches sending alerts in response to matches of said system event signatures to said intrusion signatures (Vaidya: Column 11 Line 62 – 65).

As per claim 23 and 26, Vaidya teaches each intrusion signature is associated with a respective action to perform in response to a predetermined number of said system event signatures matching said each intrusion signature (Vaidya: Vaidya: Column 11 Line 48 – 51: see the same rationale as above in claim 21).

As per claim 31 and 32, Vaidya teaches method of detecting intrusions, said method comprising the steps of:

storing a plurality of intrusion signatures (Vaidya: Column 2 Line 53 – 59);

automatically detecting a multiplicity of system events having respective signatures (Vaidya: Column 3 Line 40 – 45);

comparing each of the multiplicity of system event signatures to said plurality of intrusion signatures (Vaidya: Column 4 Line 8 – 18), one of said system event signatures not matching any of said intrusion signatures and not corresponding to an intrusion, and other of said system event signatures matching respective ones of said intrusion signatures (Vaidya: Column 3 Line 41 – 45); and storing said one system event signature in association with said plurality of intrusion signatures (Vaidya: Column 5 Line 60 – 63);

recording a number of times that said each of said intrusion signatures matches a respective one of said system event signatures (Vaidya: Column 8 Line 18 – 39);

recording a number of times that said one system event has occurred (Vaidya: Column 8 Line 18 – 39);

subsequently ordering the stored plurality of intrusion signatures and said one system event signature based on the respective number of times that have been recorded for said plurality of intrusion signatures and said one system event signature, such that the signature for which the most number of times has been recorded is first in the order (Vaidya: Column 11 Line 48 – 51: the likelihood of occurrence is based on the occurrence sequence of events during the network intrusion detection presented as in an sequential order on the list (table) of the attack signature profile – i.e. the first qualifier condition would be always can be met most of the time as the comparison goes by and stop anytime when not matched); and subsequently comparing a signature of a subsequent system event with said signatures in said order until finding a match between said subsequent system event signature and one of said signatures in said order (Vaidya: Column 11 Line 48 – 51: see the same rationale as above).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100